DARKTRACE

DATA SHEET

What Darktrace Finds

Darktrace finds anomalies that bypass other security tools, due to the uniqueness of the Enterprise Immune System, capable of detecting threats without reliance on rules, signatures or any prior knowledge.

Across our customer base, we have detected a wide range of different anomalies, detected by our probabilistic approach that takes into account weak indicators to form a compelling picture of overall threat. The following list includes examples of anomalies that we have spotted in real operational environments. For each anomaly found, the organization affected had the ability to respond to the evolving situation in the most appropriate way, in order to best protect their information and the integrity of their systems.

The examples given below name specific technical components of each anomaly. Such components are often featured in rule definitions and, for ease of interpretation, Darktrace's notifications publish each specific component whose behavior has contributed to the models' characterization of threat. Darktrace models these specific components collectively and over time. It is how these parameters behave relative to each other and to a previous epoch that determine a notification's status, unlike a rule-based system that relies on prior setting of threshold values in a single or set of discrete parameters. However, it should be noted that Darktrace can use pre-existing rules as base line or seed points for its adaptive mathematical models and this is often an option for environments where prior history does not exist.

Remote access attack linked to dangerous malware

Darktrace identified an attack on the company's corporate network using a RAT (Remote Access Tool). This appeared to be the result of activity relating to a well-known botnet, an attacker-controlled infrastructure formed of infected computers, which the attacker controls over the internet. The media reported this botnet to have been controlled by a cyber-crime group in Eastern Europe. The attackers hire out the botnet for a variety of malicious activities, including harvesting credit card details, stealing confidential corporate data and running email attacks.

This particular variant of the virus had adapted itself to avoid being detected by sandboxing defenses, as well as hiding some of its operating processes to avoid host-based security tools and anti-virus. It is an extremely clever and dynamic form of malware, which uses complex algorithms to ensure that it is not detected by legacy security tools. Darktrace was able to find traces of its presence by comparing these computers' behaviors over time.

Anomalous data transfer

Darktrace observed that a company machine was making anomalous internet connections to one IP address using the often-abused Adobe Flash software. Suspiciously, there was no evidence of this IP being resolved through DNS and the connections contained command names in the HTTP GET requests. This appeared to be a covert method of communication that an attacker had initiated, using a channel that had travelled unhindered through the company's firewall and other border defenses. Further investigation revealed this to be a malware infection.

Domain Generation Algorithm

Darktrace detected that several of a company's devices were behaving in the same anomalous manner. The devices attempted over 1,000 connections in a short period of time with randomly-generated domain names, indicating the use of a 'Domain Generation Algorithm'. This is a method commonly used by attackers to move their servers across a number of domain names, making them difficult to pinpoint by security staff, and allowing the attacker to evade detection.

Malicious web drive-by

One of the company's users was subjected to a malicious 'drive-by' attack while browsing a legitimate website about blues music. Unbeknown to the user, the machine redirected to a separate site that had recently been registered in California. Detailed analysis revealed that the domain name looked suspicious, as part of it appeared to contain another domain name in a disguised form. Subsequently, the machine also redirected to several further sites. Darktrace determined that this was unlikely to have been user behavior and suggested that malware was already installed on the device.

Suspicious Java download

While a user browsed a website about electronics, the machine was redirected to another site, which prompted the download of a malicious piece of JavaScript. This is a commonly-abused scripting language used to inject malicious content. Subsequent to this, the machine also downloaded a '.jar' file (a Java archive file) in the background, which was then used by attackers to exploit the machine. Although this file is known as malicious among the security community, the company's other defenses failed to prevent this attack.

Infection with ransomware

Darktrace detected multiple indicators of suspicious behavior on one of the organization's machines. One user was browsing a popular news website in the early hours of the morning when a suspicious search bar attached itself to the user's browser. This was probably a result of the user clicking on malicious advertising content on the page. The machine then manipulated the user's search results in the background, probably in an attempt to generate click-through revenue.

After clicking on one of these malicious links, the user was subsequently directed to a suspicious website where it made a number of further downloads. Detailed analysis revealed that the website had been registered one day prior to this activity, using apparently false details: the telephone number provided was Russian, but the address was US-based.

This activity exhibited the signs of infection with a well-known form of ransomware, a type of malware that encrypts the user's files, making them unreadable, and extorts a charge to the user for unlocking them. This posed a clear risk to the integrity of the company's data and its continued business operations. Darktrace observed that the malware had already iterated through a number of internal files containing photographs, meeting details and reports on product testing.

Bitcoin mining

Darktrace alerted the organization about unusual connections on one of the company's machines; the machine was observed regularly mining for Bitcoins, a type of electronic currency. This involved the machine sharing its computing power with a third party, in an attempt to generate new Bitcoins. The machine appeared to be part of a 'botnet', a network of multiple computers all controlled by one attacker who stood to gain by abusing the company's resources.

Use of 'Tor' anonymizing network

Darktrace identified one of the company's machines connecting to the internet over the 'Tor' network, which anonymizes and encrypts connections, providing the user with complete privacy and anonymity. Darktrace was able to bring this clear breach of company policy to the attention of the organization.

Peer-to-peer connections with the Far East

One of the company's devices was detected establishing a type of 'peer-to-peer' internet connection with servers in the Far East, occurring on three consecutive days. The machine then sent information over this obscured channel. This activity was unusual compared with the machine's normal behavior, and clearly represented a risk to the company's security. The use of this peer-to-peer connection had gone unnoticed, meaning that the company would not be aware that a third party was exfiltrating company data unobserved.

Illegitimate access to database server

Darktrace identified that one of the company's database servers was repeatedly allowing unencrypted connections from various internet locations. These machines were using a range of IP addresses allocated to a telecoms company in the Far East. Darktrace's processing of these connections suggested that the data being transferred was financial information. Attackers often target database servers for the high-value information that they hold. The direct, unencrypted communications from the internet to this server observed by Darktrace were extremely risky. The potential for leaking or changing vital financial information through this server represented a serious risk to the company's operations and reputation.

Unauthorized use of administrator credentials

Darktrace observed that a privileged user credential was repeatedly logging in to the company network at unusual times. This activity began in the early hours of the morning, finishing at around midday. Given that this user normally only logged in during the working day, this represented anomalous behavior and constituted a serious threat to the company's security, as system administrators have the most privileged level of access to company networks and data, which an attacker exploiting these credentials may have taken advantage of.

Fast travel indicating password compromise

Darktrace Cyber Intelligence Platform observed that one user's credentials were used simultaneously from two locations in Europe and East Asia. While the user may have been working remotely, this activity also suggested that the user's password may have been compromised and was being used illegitimately by a third party, perhaps even from outside the company.

Anomalous internal file transfers

Darktrace observed that one of the company's computers, located in the US, downloaded an anomalously large amount of data – up to 1GB of information. This data came from one of the company's shared folders. The behavioral model created for this machine showed that it often downloaded data in this way, but never in such large volumes. Detection of this anomaly allowed the company to take remedial action against an employee abusing their access rights.

Use of virtual Cyrillic keyboard

One of a company's devices was observed using a website that provides users with virtual Cyrillic keyboards. Darktrace observed this anomalous activity within the company's UK headquarters, which appeared suspicious, as it suggested that a remote attacker may have been attempting to change the keyboard in order to type commands in his own language.

Connections to website linked to Advanced Persistent Threats

One of the company's devices made repeated connections to servers that have been linked to Advanced Persistent Threat (APT) groups in countries in the Far East. The user was redirected from a popular social networking website through a chain of suspicious websites, while apparently viewing a compromised video. Darktrace's detection of this suspicious activity allowed the company to effectively remediate against an emerging anomaly that threatened to leak their intellectual property to foreign competitors.

Attempted connections to non-existent domain names

Darktrace detected a malware infection on three of the company's devices, due to unusual behavior exhibited by the device over a period of time. The machines were requesting a large number of non-existent domain names from an external DNS server, a process that, in this case, was used to hide malicious traffic. The company also had no record of the purpose of one of the machines, which was highly suspicious and possibly indicative of an insider threat.

Port-scanning for internal company resources

Darktrace Cyber Intelligence Platform observed that one of the company's machines was port-scanning the internal network, apparently to establish which machines were running a particular service. The machine involved was an Apple product, but was claiming to use an old version of the Windows operating system, which appeared suspicious. The port-scanning activity was also anomalous based on this machine's normal pattern of life, and suggested that an attacker was attempting to perform reconnaissance on the network before further exploitation.

Suspicious file download using XOR obfuscation

One of the company's machines was identified downloading a suspicious file from the internet into the company network. The file was in binary form but its contents were disguised using a form of obfuscation known as XOR, so its purpose was deliberately hidden. The website that provided the file has previously been known to have facilitated malware attacks. Darktrace automatically de-obfuscated the file and alerted the enterprise to the probable threat.

Risk from 'bring-your-own-device' (BYOD) policies

A user was observed downloading non-corporate email onto his personal iPhone, whilst connected to the company's corporate network. As this type of email communications is unmonitored by corporate perimeter security tools, it exposes the company to spear-phishing attacks, where attackers pose as legitimate contacts or businesses in the hope of tricking users into clicking malicious links or attachments embedded in the email. Spear-phishing attacks are well known to have a high success rate and can deliberately target personal devices, which are often less well-defended. Given that the iPhone was connected to the corporate network, any successful phishing attacks may have allowed attackers to jump from the iPhone device onto corporate resources, putting systems integrity and the company's reputation at risk.

Company Server Hijacked by Criminal Group

A server belonging to a Darktrace customer was observed participating in Distributed Denial of Service (DDoS) attacks against a range of websites, as well as being involved in suspected criminal financial deals.

The server was observed by Darktrace making multiple connections over a period of a few hours to a variety of foreign websites dedicated to online gaming. This was unusual compared to its normal everyday activities, leading the Enterprise Immune System to raise an alert. After further research, Darktrace analysts discovered that the customer server had been hijacked by a hacking

group from South-East Asia and was being used in a large-scale DDoS attack against a range of target websites. A DDoS attack involves sending the website or server a large amount of traffic in order to overload it and bring it down.

After discovering that one of the websites that was being attacked had previously been taken over by a hacking group, Darktrace was able to attribute the DDoS attack to a rival hacking organization using the hijacked customer server as a tool to take revenge on the first group.

Darktrace also observed that the same customer server was connecting to a website that facilitated criminal financial activity, indicating that the organization that had hijacked it was still in control of the server and was using it to carry out clandestine financial operations. Often, transactions of this type involve money laundering and payment for carrying out online criminal activity such as targeted attacks against both criminal and legitimate targets. Despite the fact that the attackers had bypassed its traditional security tools, Darktrace was able to alert the customer to this, enabling it to retake control of its server and prevent further use of its resources by the attackers.

About Darktrace

Named 'Technology Pioneer' by the World Economic Forum, Darktrace is one of the world's leading cyber threat defense companies. Its Enterprise Immune System technology detects previously unidentified threats in real time, powered by machine learning and mathematics developed at the University of Cambridge, which analyze the behavior of every device, user and network within an organization. Some of the world's largest corporations rely on Darktrace's self-learning appliance in sectors including energy and utilities, financial services, telecommunications, healthcare, manufacturing, retail and transportation. The company was founded in 2013 by leading machine learning specialists and government intelligence experts, and is headquartered in Cambridge, UK and San Francisco, including offices in Auckland, Boston, Chicago, Dallas, London, Los Angeles, Milan, Mumbai, New York, Paris, Seoul, Singapore, Sydney, Tokyo, Toronto and Washington D.C.

T: +44 (0) 1223 350 653 E: info@darktrace.com www.darktrace.com